E-Phishing

2022企业邮件钓鱼模拟演练分析报告

The Report Of Enterprise Phishing Simulation Practices In 2022

易念科技 | 意识决定安全 Coremail

INSec WORLD 安在 ANZER

关于报告

据知名安全媒体CSO Online的一项调查，“企业平均部署了75款来自不同安全厂商的安全工具以期保障网络安全”。然而事实上，任何企业，无论安装了多少安全硬件与软件产品，以“人”为目标、基于社会工程学的网络钓鱼攻击总是可以成功突破企业安全防线。**不在组织网络安全文化建设、全员安全意识培训及钓鱼模拟演练**上下功夫的企业，将不可避免地沦为全球黑客“宰割的羔羊”。

本报告分为宏观篇、实战篇、调研篇及展望篇，分析样本涵盖**国内14个不同行业、涉及150多家企业、近51万名受测员工、超过96万封模拟邮件**，由中国网络空间安全人才教育论坛(CEAC)网安意识工作组、易念科技、InsecWorld 世界信息安全大会、Coremail及安在新媒体联合发布，旨在洞察新数字威胁下企业开展邮件钓鱼模拟演练的需求、做法和趋势，积极探索钓鱼模拟演练最佳实践。

宏观篇

2022 全球仅35%企业开展了钓鱼模拟演练

根据 Proofpoint《2023 全球网络钓鱼攻击状态报告》

仅35%企业开展了邮件钓鱼模拟演练

仅56%%企业提供了全员安全意识培训

2022 全球初次钓鱼演练中招率最高行业

根据 Knowbe4《2022 邮件钓鱼演练行业基准报告》

小型组织 1-249人	中型组织 250-999人	大型组织 1000人以上
32.7% 教育	39.4% 医院	52.3% 保险
32.5% 医疗&制药	36.6% 医疗&制药	52.2% 咨询
31.5% 零售&批发	34% 能源与公用事业	50.9% 能源与公用事业

各行业初次演练平均中招率 **32.4%**

2022 国内十大真实钓鱼邮件主题

根据Coremail 邮件安全人工智能实验室 2022年1月1日-12月31日监测数据(排名不分先后):

1.快递到货通知

2.提升优化-邮寄系统通知

3.【电子发票】您收到一张新的电子发票

4.个人劳动补助/补贴/津贴已下发,请及时查收

5.【重要提醒】邮件数量过多,即将到达上限

6.2022年终绩效(补助)申领通知查看附件

7.邮箱账号停用通知!

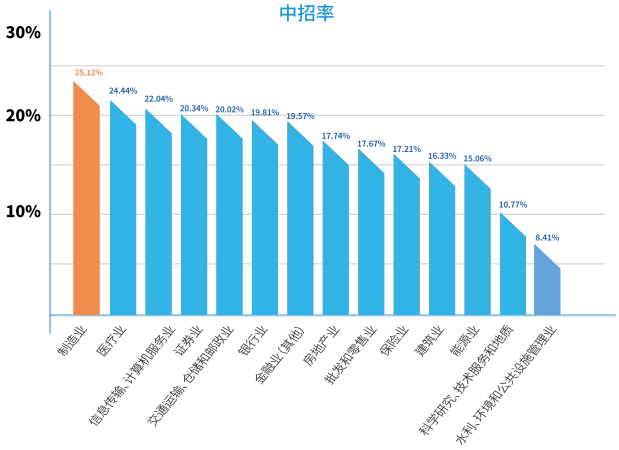
8.邮箱安全警告:您的邮箱账户已暂停收发信权限!

9.最新个人通知

10.关于帐户三天后无法使用!

实战篇

制造业钓鱼演练中招率最高 (25%)

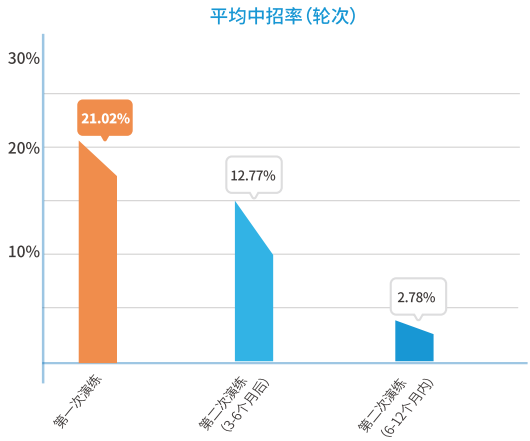


十大钓鱼演练常用邮件模板主题

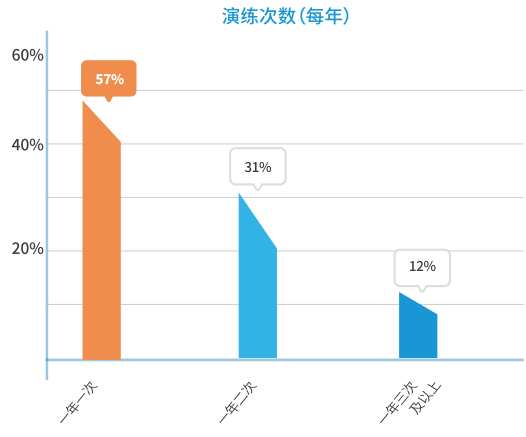
(排名不分先后)

员工薪资调整	节日放假通知
复工复产信息填报	系统异地登录通知
疫情扫描领补贴	邮件系统升级通知
钓鱼演练结果通知	密码强度监测
邮件密码修改	个人所得税退税

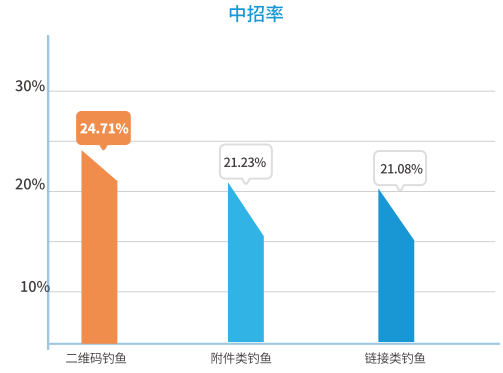
各行业平均首次钓鱼演练中招率为 (21%)



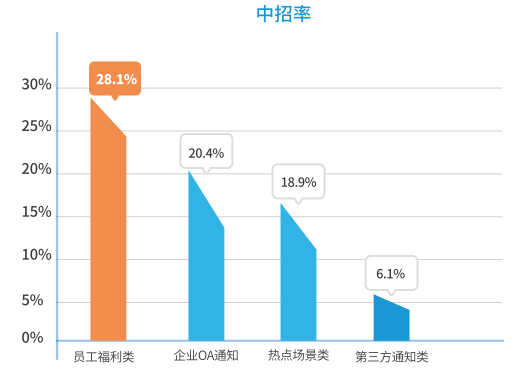
超四成企业每年至少开展2次钓鱼演练



从演练攻击类型看,二维码钓鱼中招率最高(24%)



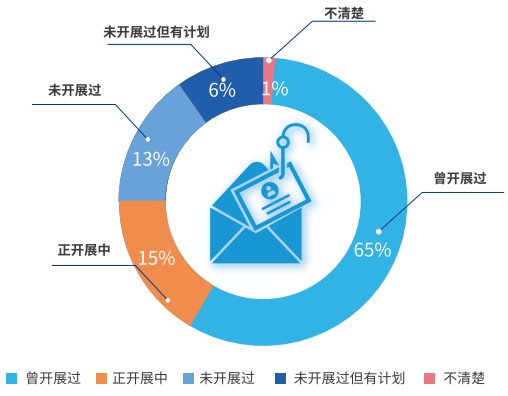
从演练模板类型看,员工福利类中招率最高(28%)



调研篇

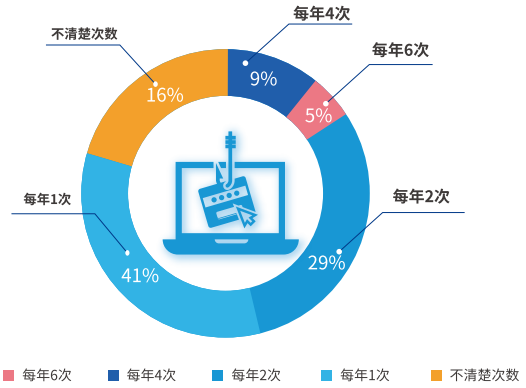
80%的受访企业开展过或正在开展钓鱼演练

开展演练比率



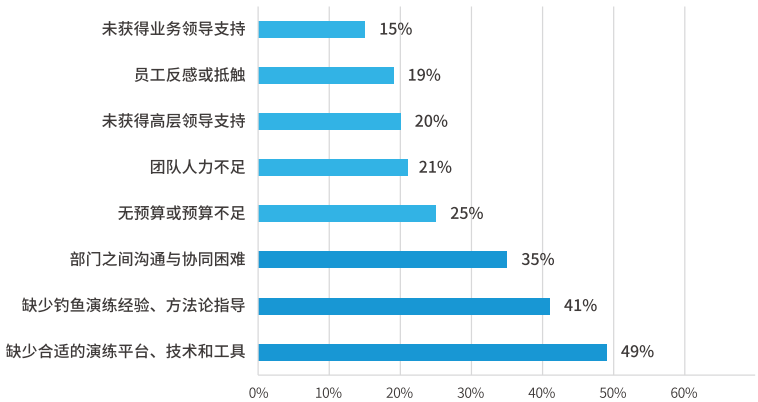
选择一年开展一次钓鱼演练的频率最高(41%)

钓鱼演练轮次



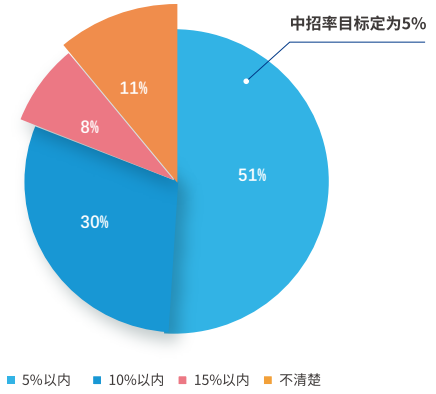
缺少合适的演练平台、技术和工具，是企业开展钓鱼模拟演练的最大阻力

最大阻力来源



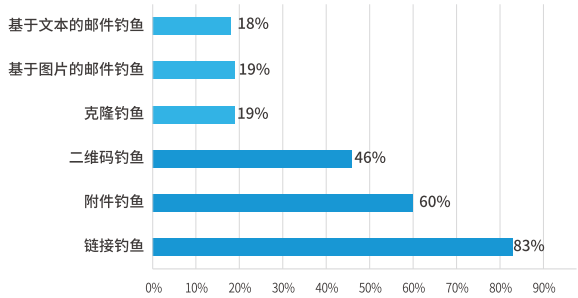
过半数企业将2023年钓鱼演练中招率目标定为5%以内

目标中招率



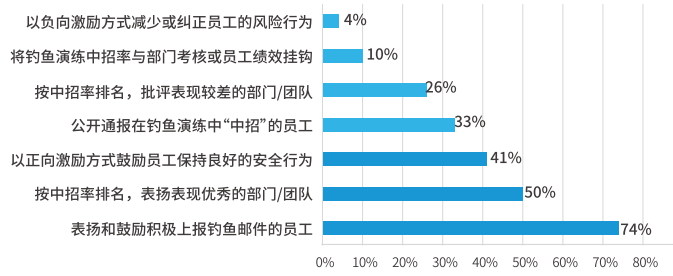
企业开展钓鱼演练最常采用的攻击类型是链接钓鱼

模拟攻击类型



“正向激励”是企业对待员工钓鱼演练表现的主要方式

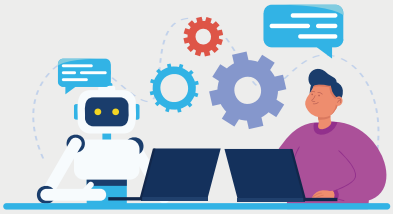
激励vs处罚



展望篇

钓鱼演练常态化 - 应对变化多端的钓鱼攻击

网络钓鱼(Phishing)始于上世纪90年代中期，时至今日，网络钓鱼仍是黑客最常用且最容易突破安全防线的一种攻击手段。只要有利可图、有“人的漏洞”可利用，针对企业和个人的钓鱼攻击便不会消失。钓鱼攻击手法千变万化，只有通过常态化开展钓鱼演练，**不断提升企业和个人的“网络安全智商”与“数字安全素养”**，才能做到知己知彼，有备无患。



钓鱼演练针对性 - 应对AI加持的钓鱼攻击

可以预见的是，利用ChatGPT等新兴技术加持的网络钓鱼攻击将愈演愈烈。在钓鱼邮件的规模、速度、效率、精准性与迷惑性方面，会给企业和个人带来更大的挑战。企业开展钓鱼演练的难度水平需要与当前员工的反钓鱼意识与能力相匹配，由**简到难逐步升级，从广撒网式过渡到鱼叉式**，最终使员工能够准确识别具有高度针对性与个性化的钓鱼邮件。

钓鱼演练游戏化 - 以正向激励释放员工潜能

据安在最新调研，**83%的受访安全人员表示愿意尝试以“游戏化”方式开展钓鱼演练**。发起贴近真实的钓鱼模拟演练固然好，但不同组织的企业安全文化成熟度不同，钓鱼演练可能会带来一定程度的“反噬效应”。而以游戏化方式开展演练，员工参与积极性更高，可以获得及时反馈与积分认可，在游戏挑战中不断磨练反钓鱼能力，成为安全团队的“好帮手”。

钓鱼演练“实践指南”

通过“**以人为本**”深化员工安全意识培训以及开展钓鱼模拟演练，是在多层级安全防御体系中，最具成本效益的一种策略。企业在计划或实施钓鱼演练时，建议综合考虑以下因素：

合理设定度量指标

打开率、点击率、中招率等关键指标固然重要，更为重要的**上报率**，反映出员工与安全团队的合作程度、安全责任感、对安全及业务的积极作用。

考虑演练难度等级

如果钓鱼演练常年停留在一个难度水平，即使得到更低的中招率也意义不大。**钓鱼演练难度应与风险等级、当前意识水平、岗位角色等相匹配**。

提前通知 or 不提前通知

两种方式各有利弊，如果不提前通知，建议**避开业务高峰期**。如果钓鱼演练以冒充内部部门身份发出，务必提前与相关部门**做好内部沟通**。

考虑员工感受 or 不考虑员工感受

虽然真实钓鱼攻击并不会照顾员工感受反而利用员工情绪，但对于演练而言，**不能为了钓鱼而钓鱼**，应即要贴近真实又要**考虑对员工感受及信任关系的负面影响**。

激励措施 or 处罚措施

虽然处罚（如通报、考核等）作为负向强化手段有一定效果，但长期而言，会破坏员工与安全团队的关系，**正向强化（如奖励、认可等）更能影响员工的行为**。

报告下载二维码

www.humanrisk.cn

专注“人为因素”风险管理